REMARKS

The applicants appreciate the careful examination the Examiner has given to this application and believe the claims as amended satisfy the Examiner's concerns.

With regard to Section 1 of the Action, the specification has been amended to add a specific reference to the prior application in which priority date has been requested.

With regard to Section 3 of the Action, the Examiner has rejected claims 1-4, 7, 9-21, 24, 26-38 under 35 U.S.C. 102(e) as being anticipated by Szymanski (US 2002/0053062 A1).

Claim 1 has been amended by introducing additional limitations to better define the invention and to further differentiate from the prior art.

Claim 1 as amended provides a method for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit. The method comprises encoding a sent data packet to form a sent encoded data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity field, and transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the sent encoded data packet being received as a received encoded data packet at the output of the transmission medium, the received encoded data packet having an "M" eight-bit bytes Protected Packet and an "n" D-parity filed, the Protected Packet comprising the sent data packet of the sent encoded data packet and a data packet of the received encoded data pack.

The method further comprises checking for errors in the data of the Protected Packet of the received encoded data packet, and if an error occurred, applying an error correction scheme for computing an error correction field for said error and inserting said error correction field in the "n" D-parity field, followed by computing, for said error correction field, an error Syndrome field having "k" error syndrome subfields. If numbers of bits in the "k" error syndrome subfields are equal,

the error correction field is applied to correct the error of the sent data packet, otherwise, the sent data packet is dropped, and then the received encoded data packet is decoded to recover a copy of the sent data packet.

The error detection scheme in the amended claim 1 addresses each byte in the data of the protected packet for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet, and if an error occurred, an error correction field is computed and inserted in the "n" D-parity field, and a corresponding error syndrome field having "k" error syndrome subfields is determined. Thus, the method of the amended claim 1 is capable of detecting and correcting a single byte which is in error, that is, it is able to correct individual bit errors when the transmission link is, e.g., a simple transmission link, as well as individual byte errors, which is necessary when a transmission link coding is used, e.g., 8B/10B line coding.

Szymanski (US 2002/0053062 A1) teaches transmitters, receivers, and coding schemes to increase data rate and decrease bit error rate of an optical data link. Data is transmitted across the link with a less than nominal bit error rate (BER) by encoding the data using a forward error correction (FEC) code or by requesting retransmission of transmitted packets in error. Data is transmitted at a speed that introduces errors at a rate that is in excess of the nominal BER but that may be corrected using the FEC code or retransmission so that the data may be received with less than the nominal BER. The data rate is increased as the link operating speed is increased beyond the overhead required by the FEC codes or retransmission.

The data of the protected packet in Szymanski (US 2002/0053062 A1) comprises the sent data packet having the FEC codes, and the error-checking scheme is used for checking errors in the sent data packet. The error-checking scheme of Szymanski (US 2002/0053062 A1) does not employ the "n" D-parity and error syndrome scheme as in the amended claims that are used to detect errors which are difficult to detect, and as a result cannot detect such errors.

Claims 2, 3, 7, 11, and 13 depend on the amended claim 1 and introduce additional limitations to better define the invention.

Claims 4, 9, 10, 12, and 14 to 17 depend on the amended claim 1.

Claim 18 is a system claim having a scope similar to the amended claim 1.

Claims 19 to 20, 22 to 25, 28, 30, 35, and 38 depend on the amended claim 18 and have additional limitations to better define the invention.

Claims 21, 26, 27, 29, 31 to 34, 36, and 37 depend on the amended claim 18.

With regard to Section 6 of the action, the Examiner has rejected claims 5-6, 22-23 under 35 U.S.C. 103(a) as being unpatenable over Szymanski (US 2002/0053062 A1) as applied to claim 3 above, and further in view of Anderson et al. (US 6,026,506).

Anderson et al. (US 6,026,506) teaches a method of concealing errors in processing a data. The method comprises detecting loss or interruption of data delivery and signaling a decoder to invoke error concealment, wherein the error is chosen from a group comprising continuity count errors, bursts of errors in consecutive transport packets, and complete loss of the transport stream. The method further comprises detecting the type of error and thereafter signaling the error type directly so that either a video frame is repeated or an audio sample is repeated or muted.

Szymanski (US 2002/0053062 A1) and Anderson et al. (US 6,026,506) combined do not teach the method of the amended claim 1. In Szymanski (US 2002/0053062 A1) and Anderson et al. (US 6,026,506) the data of the protected packet comprises the sent data packet having error correction codes such as FEC. It lacks the steps involving the "n" D-parity field and the error syndrome value that provide for detecting errors that are difficult to detect. For such errors, in a combined Szymanski (US 2002/0053062 A1) and Anderson et al. (US 6,026,506), and in contrast to the present invention, the method of the error correction may fail, and the sent data packet is dropped, followed by the re-transmission of the sent data packet.

Claims 3, 5, and 6 depend on the amended claim 1 and have been amended by introducing additional limitations to better define the invention.

Claims 22 and 23 depend on the amended claim 18 and have been amended by introducing additional limitations to better define the invention. Therefore, it is respectfully submitted that this rejection of the Examiner has been traversed.

With regard to Section 7 of the action, the Examiner has rejected claims 8, 25 under 35 U.S.C. 103(a) as being unpatenable over Szymanski (US 2002/0053062 A1) as applied to claim 2 above, and further in view of Garrabrant et al. (US 6,389,572).

Garrabrant et al. (US 6,389,572) teaches a method for correcting errors in data blocks representing a modulated waveform, the method comprising the steps of receiving an analog input signal; performing an analog to digital conversion on the signal; removing DC components from the digital result; extracting samples to fill columns of a sample table, the sample table being comprised of rows and columns of sample entries; for each row except the first row, proceeding from the top to the bottom of the sample table, creating an estimate by thresholding around the zero level; generating at least one position of an error in the sample entries; flipping the at least one bit represented by the error; performing intersymbol interference (ISI) level adjustment as derived from the previously processed row; repeating for each row in the reverse direction except the last row, as going from the bottom to the top of the sample table.

Szymanski (US 2002/0053062 A1) and Garrabrant et al. (US 6,389,572) combined do not teach the method of the amended claim 1. In Szymanski (US 2002/0053062 A1) and Garrabrant et al. (US 6,389,572) the data of the protected packet comprises the sent data packet having codes relevant to inter symbol interference (ISI). Again, the method of combined Szymanski (US 2002/0053062 A1) and Garrabrant et al. (US 6,389,572) lacks the steps involving the "n" D-parity field and error syndrome value that provide for detecting errors that are difficult to detect.

Claims 2 and 8 depend on the amended claim 1 and have been amended by introducing additional limitations to better define the invention.

Claim 25 depends on the amended claim 18 and has been amended by introducing additional limitations to better define the invention. Therefore, it is respectfully submitted that this rejection of the Examiner has been traversed.

The Examiner is requested to respectfully reconsider this application with regard to the amendments to the claims presented above and the above arguments with a view to considering the claims favorably for allowance.

The Commissioner is hereby authorized to deduct any prescribed fees for these amendments from our Company's **Deposit Account No. 501832.**

Yours truly,
Edward Aung Kyi Maung

By:________________

Victoria Donnelly, Ph.D.
Patent Agent
Reg. No. 44,185

TROPIC NETWORKS INC.,
Intellectual Property Department
135 Michael Cowpland Drive
Kanata, Ontario, Canada.
K2M 2E9

Telephone: (613) 270-6026
FAX: (613) 270-9663
E-mail: Victoria.Donnelly@tropicnetworks.com

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this paper (27 pages) is being facsimile transmitted to the U. S. Patent and Trademark Office on the date shown below.

Date: 17 November 2004

Omayma E. Moharram, Ph.D., P.Eng.
Patent Engineer,
TROPIC NETWORKS INC.,
Intellectual Property Department
135 Michael Cowpland Drive
Kanata, Ontario, Canada.
K2M 2E9

Telephone: (613) 270-6942
FAX: (613) 270-9663
E-mail: Omayma.Moharram@tropicnetworks.com

AMENDMENTS TO THE CLAIMS

CLAIMS:

1. (currently amended) A method for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the method comprising the steps of:

(a) encoding a sent data packet to form a sent encoded data packet~~,~~ ~~including:~~

~~applying an error detection scheme to the sent data packet to~~ having an "M" eight-bit bytes Protected Packet and an "n" D-parity field ~~add a first error detection field to the packet to form a first Protected Packet~~;

~~applying an error correction scheme to the first Protected Packet to add a first error correction field to said first Protected Packet to form the Sent Encoded Packet;~~

(b) transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the sent encoded data packet~~Sent Encoded Packet~~ being received as a received encoded data packet ~~Received Encoded Packet~~ at the output of the transmission medium, the received encoded data packet ~~Received Encoded Packet including a second Protected Packet and a second error correction field, the second Protected Packet including a second data packet and a second detection field~~ having an "M" eight-bit bytes Protected Packet and an "n" D-parity filed, the Protected Packet comprising the sent data packet of the sent encoded data packet and a data packet of the received encoded data packet;

(c) checking for errors in the data of the Protected Packet of the received encoded data packet, and if an error occurred, applying an error correction scheme for computing an error correction field for said error and inserting said error correction field in the "n" D-parity field;

(d) computing, for said error correction field, an error Syndrome field having "k" error syndrome subfields, and if numbers of bits in the "k" error syndrome subfields are equal, applying the error correction field to correct the error of the sent data packet, otherwise, dropping the sent data packet; and

(e) decoding the received encoded data packet ~~Received Encoded Packet~~ to recover a copy of the sent data packet.

2. (currently amended) A method as described in claim 1, wherein the step (a) ~~of decoding~~ comprises~~: correcting errors, if any, in the Received Encoded Packet to recover a third Protected Packet, the third Protected Packet having a third data packet and a third detection field, the third Protected Packet including fields from the second Protected Packet with the errors being corrected, the third Protected Packet being a copy of the first Protected Packet within the power of the correction scheme~~ encoding the sent data packet to form the sent encoded data packet having the "M" eight-bit bytes Protected Packet, wherein the Protected Packet has data fields having "x" bytes of data, and a cyclic redundancy code (CRC) field having "y" bytes such that " x + y" equals to "M".

2a. (new) A method as described in claim 2, wherein the CRC field comprises a detection field of the sent encoded data packet and a detection field of the received encoded data packet.

2b. (new) A method as described in claim 2, wherein "M"= 66, "x"= 64, and "y"=2.

3. (currently amended) A method as described in claim ~~2~~1, wherein the step (c) ~~of decoding~~ further comprises~~: determining the integrity of the third Protected Packet; and if the integrity is confirmed, recovering a recovered data packet from the third Protected Packet, the recovered data packet being a copy of the sent data packet within the power of the correction and detection schemes~~ calculating data parity in the "n" D-parity field, and wherein "n" equals to three (3).

3a. (new) A method as described in claim 3, wherein the "n" D-parity field comprises a correction field of the sent encoded data packet and a correction field of the received encoded data packet.

4. (original) A method as described in claim 2, wherein the step of correcting errors comprises correcting one or more errors occurred in a single data word of the Sent Encoded Packet only.

5. (currently amended) A method as described in claim ~~3~~1, wherein the step (d) ~~of decoding~~ comprises generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

6. (currently amended) A method as described in claim ~~3~~5, wherein the step (d) ~~of decoding~~ comprises generating a packet drop indicator signal if the integrity of the data of said Protected Packet is not confirmed.

7. (currently amended) A method as described in claim 41, wherein the step (d) ~~of applying the error correction scheme to the first Protected Packet to add the first error correction field~~ comprises applying an algebraic function to the data words in the data of said ~~first~~ Protected Packet to generate ~~the first~~ respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet.

8. (currently amended) A method as described in claim ~~2~~1, wherein the step ~~of correcting~~(d) comprises ~~the following steps~~:

(k) applying an algebraic function to the data words in the data of said ~~second~~ Protected Packet to generate ~~a third~~ respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet;

(l) applying a bitwise exclusive OR function to said generated error correction fields ~~the second and third correction fields~~ to obtain ~~an~~ corresponding error syndrome values~~;~~, and

if an error occurred, identifying the data word which has the error and obtaining a bit pattern of the error from the error syndrome values; and

(m) correcting the identified word in the data of said ~~second~~ Protected Packet by using the obtained bit pattern to obtain a corrected ~~the third~~ Protected Packet.

9. (original) A method as described in claim 7, wherein the step of applying the algebraic function comprises performing a N-dimensional parity calculation.

10. (original) A method as described in claim 9, wherein the step of applying N-dimensional parity calculation comprises performing a 3D (three dimensional) parity calculation.

11. (currently amended) A method as described in claim 1, wherein the step ~~of applying the error detection scheme~~(c) comprises applying an algebraic function to the data words in the sent data packet of the Protected Packet to generate ~~the first~~ a detection field.

12. (original) A method as described in claim 11, wherein the step of applying the

algebraic function comprises applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

13. (currently amended) A method as described in claim ~~3~~7, wherein the step of determining the integrity of the data of said Protected Packet comprises:

(n) applying said error detection scheme to ~~the third~~ the data of the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet of said Protected Packet ~~packet~~ to generate ~~a fourth~~ respective detection fields;

(p) comparing the ~~third and fourth~~ generated detection fields; and

(q) confirming the integrity of the ~~third~~ data of the Protected Packet, if the ~~third and fourth~~ generated detection fields are equal.

14. (original) A method as described in claim 10, wherein the transmitting of data is performed so that each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

15. (original) A method as described in claim 1, wherein transmitting of the sent encoded data packet through the transmission medium comprises transmitting said packet through the transmission link.

16. (original) A method as described in claim 15, wherein transmitting the sent encoded data packet through the transmission link comprises transmitting said packet through the link which provides line coding of the transmitted data.

17. (original) A method as described in claim 16, wherein the transmitting the packet through the line coded link comprises transmitting the packet through the link, which provides 8B/10B line coding.

18. (currently amended) A system for transmitting digital data in a form of packets through a

transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the system comprising:

(1) ~~means~~ an encoder, ~~for~~ encoding a sent data packet to form a sent encoded data packet~~, including:~~

~~means for applying an error detection scheme to the sent data packet to add a first error detection field to the packet to form a first Protected Packet~~ having an "M" eight-bit bytes Protected Packet and an "n" D-parity field;

~~means for applying an error correction scheme to the first Protected Packet to add a first error correction field to said first Protected Packet to form the Sent Encoded Packet;~~

(2) ~~means~~ a transmitter, ~~for~~ transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the sent encoded data packet ~~Sent Encoded Packet~~ being received as a received encoded data packet ~~Received Encoded Packet~~ at the output of the transmission medium, the received encoded data packet ~~Received Encoded Packet including a second Protected Packet and a second error correction field, the second Protected Packet including a second data packet and a second detection field; and~~ having an "M" eight-bit bytes Protected Packet and an "n" D-parity filed, the Protected Packet comprising the sent data packet of the sent encoded data packet and a data packet of the received encoded data packet;

(3) a detector, checking for errors in the data of the Protected Packet of the received encoded data packet, and if an error occurred, applying an error correction scheme for computing an error correction field for said error and inserting said error correction field in the "n" D-parity field;

(4) a corrector, computing, for said error correction field, an error Syndrome field having "k" error syndrome subfields, and if numbers of bits in the "k" error syndrome subfields are equal, applying the error correction field to correct the error of the sent data packet, otherwise, dropping the sent data packet; and

(5) ~~means~~ a decoder, ~~for~~ decoding the received encoded data packet ~~Received Encoded Packet~~ to recover a copy of the sent data packet.

19. (currently amended) A system as described in claim 18, wherein the ~~means~~ corrector ~~for decoding~~ comprises~~:~~ means for correcting errors ~~in the Received Encoded Packet to recover a third Protected Packet, the third Protected Packet having a third data packet and a third detection field, the third Protected Packet including fields from the second Protected Packet with the errors being corrected, the third Protected Packet being a copy of the first Protected Packet within the power of the correction scheme~~ in the data of the Protected Packet of the received encoded data packet.

19a. (new) A system as described in claim 18, wherein the detector comprises means for calculating data parity in the "n" D-parity field, and wherein "n" equals to three (3).

20. (currently amended) A system as described in claim 19, wherein the ~~means~~ corrector ~~for decoding~~ further comprises~~:~~ means for ~~determining the integrity of the third Protected Packet; and means for recovering a recovered data packet from the third Protected Packet, the recovered data packet being a copy of the sent data packet within the power of the correction and detection schemes~~ storing the "M" eight-bit bytes Protected Packet in a two-dimensional array of bytes.

20a. (new) A system as described in claim 20, wherein the corrector has a random access memory for storing the two-dimensional array of bytes of the "M" eight-bit bytes Protected Packet.

21. (original) A system as described in claim 19, wherein the means for correcting errors comprises means for correcting one or more errors occurred in a single data word of the Sent

Encoded Packet only.

22. (currently amended) A system as described in claim ~~20~~18, wherein the ~~means~~ corrector ~~for decoding~~ comprises means for generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

23. (currently amended) A system as described in claim ~~20~~22, wherein the ~~means~~ corrector ~~for decoding~~ further comprises means for generating a packet drop indicator signal if the integrity of the ~~third~~ data of said Protected Packet is not confirmed.

24. (currently amended) A system as described in claim ~~21~~22, wherein the ~~means~~ corrector ~~for applying the error correction scheme to the first Protected Packet to add the first error correction field~~ comprises means for applying an algebraic function to the data words in the ~~first~~ data of said Protected Packet to generate ~~the first~~ respective error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet.

25. (currently amended) A system as described in claim ~~19~~18, wherein the ~~means for correcting~~corrector comprises:

(w) means for applying an algebraic function to the data words in the ~~second~~ data of said Protected Packet to generate ~~a third~~ error correction fields for the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet, respectively;

(x) means for applying bitwise exclusive OR function to ~~the~~ said ~~second and third~~ generated -error correction fields to obtain ~~an~~ corresponding error syndrome values;

(y) means for identifying the data word which has the error, if any, and means for obtaining a bit pattern of the error from the error syndrome values; and

(z) means for correcting the identified word in the ~~second~~ data of said Protected Packet by using the obtained bit pattern to obtain ~~the third~~ a corrected Protected Packet.

26. (original) A system as described in claim 24, wherein the means for applying the algebraic function comprises means for performing a N-dimensional parity calculation.

27. (original) A system as described in claim 26, wherein the means for performing the N-dimensional parity calculation comprises means for performing a 3D (three dimensional) parity calculation.

28. (currently amended) A system as described in claim 18, wherein the ~~means~~ detector ~~for applying the error detection scheme~~ comprises means for applying an algebraic function to the data words in the sent data packet of the Protected Packet to generate ~~the first~~ a detection field.

29. (original) A system as described in claim 28, wherein the means for applying the algebraic function comprises means for applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

30. (currently amended) A system as described in claim ~~20~~25, wherein the means for determining the integrity of the data of said Protected Packet comprises:

(i) means for applying said error detection scheme to ~~the~~ said ~~third~~ data of the sent data packet of the sent encoded data packet and the data packet of the received encoded data packet of said Protected Packet ~~packet~~ to generate ~~a fourth~~ respective detection fields;

(ii) means for comparing the ~~third and fourth~~ generated detection fields; and

(iii) means for confirming the integrity of the ~~third~~ data of the Protected Packet, if the ~~third and fourth~~ generated detection fields are equal.

31. (original) A system as described in claim 27, wherein each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

32. (original) A system as described in claim 18, wherein the transmission medium comprises a transmission link.

33. (original) A system as described in claim 32, wherein the transmission link comprises a line encoder for transforming each "p" bits of said sent encoded data packets into "q" bits, "q" being not less than "p", and a line decoder for transforming each of the received "q" bits into "p" bits of said received encoded data packets.

34. (original) A system as described in claim 33, wherein "p"=8 and "q"=10.

35. (currently amended) An encoder for ~~a~~ the system described in claim 18 ~~transmission system~~ for transmitting digital data in a form of packets through a transmission medium with error correction, comprising:

(6) ~~means for~~ a detector, adding an error detection field to the Protected Packet of the ~~to a~~ sent encoded data packet ~~to form a Protected Packet~~;

(7) ~~means for~~ a corrector, adding ~~an~~ a respective error correction field to the Protected Packet ~~to form an~~ of the -sent encoded data packet; and

(8) ~~means for~~ a transmitter, sending the sent encoded data packet to the transmission medium.

36. (original) An encoder as described in claim 35, wherein the means for adding the error detection field comprises means for adding the error detection filed according to one the schemes: CRC-16, CRC-32 and checksum.

37. (original) An encoder as described in claim 35, wherein the means for adding the error correction field comprises means for applying 3D parity calculation to the Protected Packet.

38. (currently amended) A decoder for ~~a transmission~~ the system described in claim 18 for ~~transmitting~~ receiving digital data in a form of packets ~~through~~ from ~~a~~ the transmission medium with error correction, the decoder ~~receiving~~ comprising:

(iv) ~~means~~ a receiver, ~~for~~ receiving a the ~~Received Encoded Packet~~ received encoded data packet from the transmission medium~~,~~;

~~the Received Encoded Packet being the encoded packet encoded by the encoder of claim 35 and transmitted through the transmission medium, Received Encoded Packet including a Protected Packet and an error correction field~~; and

(v) ~~means~~ a corrector, ~~for~~ correcting errors, if any, in the received encoded data packet ~~Received Encoded Packet~~ to recover a corrected Protected Packet which includes fields from the Protected Packet with the errors being corrected; and

(vi) ~~means for~~ a detector, determining integrity of the data of the corrected Protected Packet; and

~~means for~~ recovering a corrected data packet from the corrected data of the Protected Packet, the corrected data packet being a copy of the sent data packet.

End of Fax 28/2